Appl. No. 09/736,688
Amdt. dated July 13, 2004
Reply to Office action of May 5, 2004

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1.   (Original) A cryptographic system in a computer system, the cryptographic system comprising:

a central server;

a remote server;

a database on the central server responsive to signals from the central server, the database being configured to contain sensitive Information;

enterprise credentials stored in the database;

a key repository process on the central server, the key repository process having one or more master keys for managing information in the database, the key repository process further configured to access the enterprise credentials and to authenticate authorizations to access the sensitive information in the database;

an agent on the remote server, the agent acting on behalf of the key repository process on the central server; and

at least one application on the remote server;

wherein the agent authenticates authorizations of specific applications to access resources based upon authorizations held and maintained by the key repository process on the central server.

2.   (Original) A cryptographic system as in claim 1, wherein the key repository process and the agent communicate with each other, the communication being authenticated by a shared secret, and wherein the shared secret is protected by a level of trust equivalent to that with which the shared secret is protected on the central server by the key repository process.

Appl. No. 09/736,688
Amdt. dated July 13, 2004
Reply to Office action of May 5, 2004

3.   (Original) A cryptographic system as in claim 2, wherein the level of trust is defined as the number of individuals required for reconstructing the master key and/or for performing a sensitive operation.

4.   (Original) A cryptographic system as in claim 1, wherein the agent in the remote server is an independent key repository process with a level of trust equivalent to that of the key repository process in the central server.

5.   (Original) The cryptographic system of claim 1, wherein at least one master key protects the sensitive information in the database.

6.   (Original) The cryptographic system of claim 1, wherein at least one master key provides privacy protection to the sensitive information.

7.   (Original) A method used in a cryptographic system for obtaining sensitive information, comprising:
   storing enterprise credentials in a database on a central server, the database being configured to contain sensitive information;
   establishing one or more master keys for managing information in the database by a key repository process, the key repository process being configured to access the enterprise credentials;
   authenticating, by the key repository process, authorizations to access the sensitive information in the database;
   establishing communications between the key repository process on the central server and an agent on a remote server, the agent acting on behalf of the key repository process on the central server; and
   authenticating, by the agent, authorizations of specific applications on the remote server to access resources based upon authorizations held and maintained by the key repository process on the central server.

8.   (Cancelled).

Appl. No. 09/736,688
Amdt. dated July 13, 2004
Reply to Office action of May 5, 2004

9.   (Previously presented) A system comprising:

a central server containing a cryptographically protected database and configured to execute a key repository process that controls access to the database; and

a remote server communicatively coupled to the central server, the remote server configured to execute an agent process that acts on behalf of the key repository process, and the remote sever further configured to execute an application program;

wherein the agent process acts on behalf of the key repository process to authenticate authorization of the application program to access the cryptographically protected database.

10.   (Previously presented) The system as defined in claim 9 wherein the agent process is an independent key repository process with a level of trust equivalent to that of the key repository process of the central server.

11.   (Previously presented) A system comprising:

a remote server configured to communicatively couple to a central server;

an agent process on the remote server, wherein the agent process acts on behalf of a key repository process executing on a central server; and

application program on the remove server;

wherein the agent process is configured to authenticate authorization of the application program on behalf of the key repository process to access a cryptographically protected database on the central server.

12.   (Previously presented) The system as defined in claim 11 wherein the agent process in the remote server configured to be an independent key repository process with a level of trust equivalent to that of the key repository process of the central server.

13.   (Previously presented) A system comprising:

a central server;

a database on the central server configured to contain sensitive information; and

a key repository process on the central server, the key repository process having one or more master keys for managing information in the database and to authenticate authorizations to access the sensitive information in the database by applications on remote servers.

14.   (Previously presented) The system of claim 13 wherein the key repository process authenticates authorizations to access the sensitive information at least in part by way of an agent process executing on the remote server.

15.   (Previously presented) The system of claim 13 wherein at least one master key protects the sensitive information in the database.

16.   (Previously presented) The system of claim 13 wherein at least one master key provides privacy protection to the sensitive information.